Department of Homeland Security Daily Open Source Infrastructure Report for 11 September 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports that Chase Card Services mistakenly threw out as trash personal information on 2.6 million past and current Circuit City credit card holders. (See item 10)
- CNN reports that a lengthy video statement from Ayman al−Zawahiri, issued on the eve of the fifth anniversary of al Qaeda's attacks on the United States, calls on Muslims to step up their resistance to the United States and warns that "new events" are on the way. (See item 44)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *September 08, Houston Chronicle (TX)* — **Lawmakers rebuke BP executives over missteps.** During a hearing Thursday, September 7, BP America's top executives were rebuked by lawmakers for a string of missteps, which preceded a major March oil leak in Alaska. House members seemed perplexed that the energy giant had failed to do a common check for pipeline corrosion for several years, even after a draft audit ordered by Alaska recommended the procedure. BP America's chairman and president, Robert Malone, and BP's Alaska chief, Steve Marshall, were queried about the company's failure to heed warnings from employees about potential pipeline corrosion. They were also asked about allegations that the company sought to intimidate employees who voiced concerns and arm−twisted an auditing company to whitewash

a report that warned about corrosion years before the leak. Company officials said their preliminary investigations into what went wrong did not confirm those allegations. The company executives did say that the partial shutdown of its Alaska pipelines should be lifted by the end of October after bypass lines and further corrosion checks are completed.
Source: http://www.chron.com/disp/story.mpl/business/4171625.html

2. *September 07, Vermont Guardian* — **Feds find radioactive particles in Vermont Yankee shipment.** A pair of dust−sized "hot particles" and a metal sliver inadvertently shipped from Vermont Yankee to a Pennsylvania nuclear reactor registered radioactivity far in excess of federal limits, regulators said Thursday, September 7. The material was in a container shipped August 31 from Vermont Yankee (VY) to the reactor in Berwick, PA. Measured by VY officials before it left Vernon, VT, the container registered approximately 60 millirem per hour of radiation, well below the Department of Transportation's (DOT) contact dose limit of 200 millirem per hour. However, by the time Susquehanna workers scanned the steel container at about 8 a.m. EST on September 1, it registered 820 millirem per hour, more than four times the DOT limit. The discovery calls into question how Vermont Yankee surveyed the shipment before it left Vernon on August 31 and how the particles managed to avoid detection. The Nuclear Regulatory Commission's David Pelton said plant officials plan to conduct a rigorous investigation of the incident, which he characterized as unusual.
Source: http://www.vermontguardian.com/local/092006/VYShipmentUpdate .shtml

3. *September 07, Associated Press* — **Enron sells last energy platform.** Enron Corp. has completed the sale of Prisma Energy International Inc. to Ashmore Energy International Ltd. Prisma Energy was the last of three major platforms under the Bankruptcy Plan to be sold or distributed to Enron's creditors. It was formed to own and operate a number of Enron's international energy infrastructure businesses.
Source: http://www.chron.com/disp/story.mpl/ap/fn/4170153.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *September 09, Philadelphia Inquirer* — **Overturned tractor−trailer leaks chemical on New Jersey highway ramp.** A tractor−trailer overturned Friday, September 8, in South Jersey near the Commodore Barry Bridge, spilling a small amount of a chemical substance. The accident occurred on the northbound ramp for Route 130 from Route 322 East in the Bridgeport section of Logan Township, NJ. The ramp remained closed into the evening.
Source: http://www.philly.com/mld/inquirer/news/local/states/new_jer sey/15477599.htm

5. *September 09, Portsmouth Herald (NH)* — **Homes evacuated due to propane leak.** A propane tank was struck by a backhoe at a home under construction at 427 South Road in Rye, NH, Friday, September 8. As a result, some homes adjacent to the incident were evacuated.
Source: http://www.seacoastonline.com/news/09092006/nhnews−ph−r−gas. leak.html

6. *September 07, WBEN 930 AM (NY)* — **Chemical spill prompts lockdown of nearby school.** A chemical spill at a manufacturing plant in North Collins, NY, Thursday, September 7, forced

the evacuation of the plant, and the lockdown of a nearby school. Two hundred and fifty gallons of hydrochloric acid spilled inside the Crescent Manufacturing plant due to valve failure.
Source: http://www.wben.com/news/fullstory.php?newsid=05760

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

7. *September 08, Palm Beach Post (FL)* — **Man arrested in ATM scheme.** Port St. Lucie, FL police arrested a man on more than 400 charges in connection with last month's ATM fraud at First Peoples Bank on Port St. Lucie Boulevard. Police believe Johnathen Sardone used European phone cards to make 200 withdrawals between August 26 and August 28, stealing more than $20,000 from credit card holders in London. Investigators said last week, before making the arrest, that the person making the withdrawals likely used a skimming device to capture information from credit cards and then used software to transfer that information onto the magnetic strips on phone cards. Surveillance video showed that the suspect spent hours at the ATM during nighttime trips, taking out $100 at a time because of limits on foreign accounts. Bank employees recognized the fraud after the ATM captured several phone cards and the bank's balance sheets reflected a high volume of transactions.
Source: http://www.palmbeachpost.com/localnews/content/local_news/epaper/2006/09/08/m3c_slatm_0908.html?cxtype=rss&cxsvc=7&cxcat =17

8. *September 07, ZDNet News* — **Credit card companies form security council.** The five major credit card companies have teamed up in the interest of better security. American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International announced Thursday, September 7, the creation of an organization to develop and maintain security standards for credit and debit card payments. The newly formed Payment Card International (PCI) Security Standards Council will manage the PCI Data Security Standard, established in January 2005 to make its implementation more efficient for all parties involved in a payment card transaction. These include merchants, payment processors, point−of−sale vendors, financial institutions, and more than a billion card holders worldwide. Standards include instructions on proper data encryption, common technical standards, and security audit procedures. The council's first action was to update the PCI security standard. The revision gives instructions for how to implement the new standards and clarifies language that was previously considered vague.
Source: http://news.zdnet.com/2100−1009_22−6113512.html

9. *September 07, Bloomberg* — **Chicago evacuation drill moves 4,000 financial district workers.** Chicago emergency officials performed an evacuation drill involving 4,000 financial district employees Thursday, September 7, the first such test by a major U.S. city to prepare for

a terrorist attack or natural disaster. The participants work in four office buildings near the corner of Wacker Drive and Monroe Street. They include employees of the Chicago Mercantile Exchange and Deloitte & Touche LLP. The drill used an evacuation scenario that would follow an explosion, said Cortez Trotter of the Office of Emergency Management and Communications. Unlike fire drills where participants are merely evacuated, the exercise was designed to have office workers walk several blocks from the intersection after the buildings were cleared. The evacuation drill was scheduled to take less than two hours and be videotaped to instruct emergency officials and residents in evacuation procedures.
Source: http://www.bloomberg.com/apps/news?pid=20601103&sid=aD7v9BJQwaw8&refer=us

10. *September 07, Reuters* — **Chase throws out personal information on 2.6 million credit card holders.** Personal information on 2.6 million past and current Circuit City credit card holders was mistakenly thrown out as trash by Chase Card Services, a division of J.P. Morgan Chase. Chase Card Services issues bank−branded and private−label credit cards for Circuit City. The company said Thursday, September 7, that it believes the tapes, inside a locked box, were compacted, destroyed, and buried in a landfill. Chase has begun notifying customers and monitoring affected accounts, but the company says it has not identified any misuse of personal information. No other Chase accounts are involved in this incident, the bank said.
Source: http://www.foxnews.com/story/0,2933,212739,00.html

11. *September 07, Websense Security Labs* — **Multiple Phishing Alert: Nordea, Apple Bank for Savings.** Websense Security Labs has received reports of a phishing attack that targets customers of Nordea, a financial services group in the Nordic and Baltic region. Users receive a spoofed e−mail message claiming that a new security system has been implemented, and that account details must be verified. The e−mail provides a link to a phishing site that attempts to collect user account information. Another report of a phishing attack target customers of Apple Bank for Savings, which is based in New York. Users receive a spoofed e−mail message claiming that their account has been suspended, and that the card associated with the account cannot be used until it is reactivated. The e−mail provides a link to a phishing site that attempts to collect the user's account information.
Screenshots: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =605
http://www.websensesecuritylabs.com/alerts/alert.php?Ale rtID=606
Source: http://www.websensesecuritylabs.com/

12. *September 07, Grand Rapids Press (MI)* — **Fumes cause evacuation of bank.** Up to 40 Fifth Third bank employees may have missed work on Thursday, September 7, after fumes from a roofing project were pumped into an operations center Wednesday, sending 16 to area hospitals and evacuating nearly 600 others. An adhesive mixed with acetone produced a noxious odor that had dozens of workers complaining of difficulty breathing, dizziness, and eye irritation when they were overcome inside the bank's 1830 East Paris Ave. SE operations center, Kentwood Fire Captain Dale Boersma said. No one suffered serious symptoms, and those who fell ill were treated with oxygen at hospitals and released. Firefighters enacted a mass casualty plan as a precaution, but the severity of the situation lessened when emergency workers realized only minor symptoms were present. At least a dozen ambulances were called to the scene and Grand Rapids sent a fire engine crew to help, Boersma said.
Source: http://www.mlive.com/printer/printer.ssf?/base/news−32/11576

40975180000.xml&coll=6

[Return to top]

Transportation and Border Security Sector

13. *September 09, Boston Herald (MA)* — **Security breach at Logan: State Police look for explosives misplaced in training exercise.** Veteran aviation security specialists called the loss of a powerful Semtex plastic explosive device at Logan International Airport in Boston, MA this week the result of “sloppy police work” by state troopers who should never have taken their eyes off the volatile material. The troopers say they did not notice when a Massport worker drove away in an agency truck to which eight ounces of Semtex had been affixed as part of an effort to train bomb−sniffing K−9 dogs. The lost explosive was thought to be somewhere along Harborside Drive, which is surrounded by a security fence and juts into an airfield near Runway 4L. Airplane traffic and airport operations were unhindered by the Semtex snafu, and safety expert Douglas Laird called that a good response.
Source: http://news.bostonherald.com/localRegional/view.bg?articleid =156652

14. *September 08, Government Accountability Office* — **GAO−06−916: Truck Safety: Share the Road Safely Pilot Initiative Showed Promise, but the Program's Future Success is Uncertain (Report).** In 2004, over 5,000 people died on our nation’s roads in crashes involving large trucks. The Department of Transportation’s (DOT) Federal Motor Carrier Safety Administration (FMCSA) operates truck safety programs, including Share the Road Safely (STRS), which has a goal to improve driving behavior around large trucks. At congressional direction, the National Highway Traffic Safety Administration (NHTSA) assumed responsibility for funding STRS in 2004, but returned STRS to FMCSA in 2006. The current transportation authorization bill requested the Government Accountability Office (GAO) to update its 2003 evaluation of STRS. This report describes the STRS initiatives DOT has implemented since 2003 and their design, reviews evaluations of STRS initiatives, and assesses DOT’s plans for the future of STRS. GAO interviewed DOT and state officials, and reviewed program plans and evaluations. GAO recommends that the Secretary of Transportation develop a strategy for expanding TACT−like (Ticketing Aggressive Cars and Trucks) initiatives, and determine the best method for using DOT’s resources and expertise to modify driver behavior. DOT officials clarified and updated information in a draft of this report and generally agreed with the recommendations.
Highlights: http://www.gao.gov/highlights/d06916high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−916

15. *September 08, Government Accountability Office* — **GAO−06−946: Natural Gas Pipeline Safety: Integrity Management Benefits Public Safety, but Consistency of Performance Measures Should Be Improved (Report).** The Pipeline Safety Improvement Act of 2002 established a risk−based program for gas transmission pipelines −− the integrity management program. The program requires operators of natural and other gas transmission pipelines to identify “high consequence areas” where pipeline incidents would most severely affect public safety, such as those occurring in highly populated or frequented areas. Operators must assess pipelines in these areas for safety risks and repair or replace any defective segments. Operators must also submit data on performance measures to the Pipeline and Hazardous Materials Safety

Administration (PHMSA). The 2002 act also directed the Government Accountability Office (GAO) to assess this program's effects on public safety. Accordingly, GAO examined the effect on public safety of the integrity management program, and PHMSA and state pipeline agencies' plans to oversee operators' implementation of program requirements. To fulfill these objectives, GAO interviewed 51 gas pipeline operators and surveyed all state pipeline agencies. GAO recommends revisions to PHMSA's performance measures to improve the agency's ability to determine the impact of the program over time. The Department of Transportation generally agreed with the report's findings and recommendations.
Highlights: http://www.gao.gov/highlights/d06946high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−946

16. *September 08, Government Accountability Office* — **GAO−06−945: Natural Gas Pipeline Safety: Risk−Based Standards Should Allow Operators to Better Tailor Reassessments to Pipeline Threats (Report).** The Pipeline Safety Improvement Act of 2002 requires that operators assess gas transmission pipeline segments in about 20,000 miles of highly populated or frequently used areas by 2012 for safety threats, such as incorrect operation and corrosion (called baseline assessments); remedy defects; and reassess these segments at least every seven years. Under the Pipeline and Hazardous Materials Safety Administration's (PHMSA) regulations, operators must reassess their pipeline segments for corrosion at least every seven years and for all safety threats at least every 10, 15, or 20 years, based on industry consensus standards −− and more frequently if conditions warrant. Operators must also carry out other prevention and mitigation measures. To meet a requirement in the 2002 act, this study addresses how the results of baseline assessments and other information inform us on the need to reassess gas transmission pipelines every seven years and whether inspection services and tools are likely to be available to do so, among other things. In conducting its work, the Government Accountability Office contacted 52 operators that have carried out about two−thirds of the baseline assessments conducted to date.
Highlights: http://www.gao.gov/highlights/d06945high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−945

17. *September 07, Aero−News* — **FAA issues safety publication in reaction to recent Comair accident.** The Federal Aviation Administration, in an apparent urge to "do something" after last month's Comair Flight 5191 tragedy, has published Safety Alert For Operators (SAFO) 06013 containing suggestions and recommendations for training programs. Although no specific mention is made of Flight 5191, background for the alert refers to the "recent tragic accident of a commuter jet taking off from the wrong runway." In what might be considered a preview of findings, the alert notes that "many airports are involved with construction projects that result in changing environments."
SAFO 06013: http://www.faa.gov/other_visit/aviation_industry/airline_operators/airline_safety/safo/all_safos/media/2006/safo06013.pd f
Source: http://www.aero−news.net/index.cfm?ContentBlockID=21f1afff−7f78−48d8−898c−fd0dec29d289&

18. *September 07, Government Accountability Office* — **GAO−06−1090T: Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program (Testimony).** The Visa Waiver Program enables citizens of 27 countries to travel to the U.S. for tourism or business for 90 days or less without obtaining a visa. In fiscal year 2005, nearly

16 million people entered the country under the program. After the 9/11 terrorist attacks, the risk that aliens would exploit the program to enter the U.S. became more of a concern. This testimony discusses the Government Accountability Office's (GAO) recent report on the Visa Waiver Program. Specifically, it describes the Visa Waiver Program's benefits and risks; examines the U.S. government's process for assessing potential risks; and assesses the actions taken to mitigate these risks. GAO met with U.S. embassy officials in six program countries and reviewed relevant procedures and reports on participating countries. GAO made a series of recommendations to the Department of Homeland Security to strengthen its ability to assess and mitigate the program's risks, such as providing more resources to the program's monitoring unit and issuing standards for the reporting of lost and stolen passport data. GAO also stated that Congress should consider establishing a deadline for the mandated biennial report to Congress.
Highlights: http://www.gao.gov/highlights/d061090thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−1090T

19. *September 07, Associated Press* — **Northwest recalls furloughed flight attendants.** Northwest Airlines is recalling all 1,131 furloughed flight attendants, in a move that will boost the size of its cabin staff as it awaits a judge's ruling on whether those workers can strike. Northwest, which is reorganizing under bankruptcy protection, said the recalled workers will fill permanent vacancies beginning September 30. "The current vacancies are created by a number of factors, including some modest operational growth and flight attendant attrition," the airline said Wednesday, September 6, after the union announced the recalls in a hotline message.
Source: http://www.usatoday.com/travel/flights/2006−09−07−nwa−attend ants_x.htm

20. *September 07, Associated Press* — **United introduces new boarding equipment.** Looking to improve its boarding process and turnaround times, United Airlines is rolling out new automated boarding equipment that it says should make getting on and off its planes much faster. The carrier put the first of five advanced jet bridges in place Thursday, September 7 at Denver International Airport in Denver, CO, one of its five U.S. hubs, with plans to install them at other airports in "the near future." The dual−end or Y−shaped bridge connects to both doors of a narrow−body plane, arching over the wing to the back door, to allow for simultaneous loading or unloading. They automatically connect to aircraft using sensors that detect the plane's position, thus doing away with the need for workers to connect them by hand. United says the bridge can reduce the time it takes to unload and then reboard a plane, by 10 minutes, allowing it to fly its planes longer each day.
Source: http://www.usatoday.com/travel/flights/2006−09−07−united−boa rding−equipment_x.htm

[Return to top]

Postal and Shipping Sector

21. *September 09, Beaumont Enterprise (TX)* — **Large envelope with powdery substances opened at Lamar University.** The student services building at Lamar University in Texas was closed and a hazardous materials team deployed following an employee opening a large envelope containing two plastic bags with powdery substances Friday afternoon, September 8.

A preliminary test suggests the substances are biological agents and ten people who could have been exposed were given antibiotics.
Source: http://www.southeasttexaslive.com/site/news.cfm?newsid=17172588&BRD=2287&PAG=461&dept_id=512588&rfi=6

[Return to top]

Agriculture Sector

22. *September 08, Stop Soybean Rust News* — **Two South Carolina soybean sentinel plots positive for rust.** Asian soybean rust was confirmed on soybeans in two more South Carolina counties Friday, September 8, including one in Sumter with the highest initial severity found to date in the state. Both finds, in Sumter and Hampton counties, were in soybean sentinel plots. South Carolina has five positive counties. The U.S. now has 45 rust−positive counties and parishes.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=945

23. *September 08, Animal and Plant Health Inspection Service* — **Implementation of chronic wasting disease rule delayed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is delaying implementation of a final rule that establishes regulations for a chronic wasting disease (CWD) herd certification program to help eliminate the disease from farmed and captive cervids in the U.S. The rule originally had an effective date of October 19. Recently, however, APHIS received petitions from several organizations representing various state agencies requesting a delay in the effective date of the CWD rule and reconsideration of several requirements. The final rule establishes a voluntary certification program for owners of deer, elk, and moose herds who chose to participate and follow requirements for animal identification, testing, herd management, and movement of animals into and from herds. The final rule also contains new requirements regarding the interstate movement of farmed cervids to prevent the spread of CWD.
CWD information: http://www.cwd−info.org/
Source: http://www.aphis.usda.gov/newsroom/content/2006/09/cwddelay. shtml

24. *September 08, Agence France−Presse* — **Netherlands on the alert after new cases of sheep disease.** Dutch agricultural authorities placed the entire country under a special regime after the discovery of two new cases of bluetongue disease. The Netherlands have notably stepped up export restrictions for cattle, sheep, and goats. The latest cases were two infected cows in the northern province of Friesland. The first cases of bluetongue disease were reported in the Netherlands in mid−August and the disease has since been identified in Belgium, France, and Luxemburg. Bluetongue is frequently reported in southern Europe but the outbreak is the first in northern Europe.
Bluetongue information: http://www.fao.org/AG/AGAINFO/subjects/en/health/diseases−cards/bluetongue.html
Source: http://news.yahoo.com/s/afp/20060908/hl_afp/netherlandsfarmhealth_060908183540;_ylt=As__eKsE6Nx6iGpxOyLWneKJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

25. *September 07, Stop Soybean Rust News* — **Three Georgia counties have new soybean rust infections on kudzu.** Georgia officials reported finding Asian soybean rust on kudzu in three southwest Georgia counties −− all appear to be "new" infections after recent rains. The samples were collected September 5 in Seminole, Grady, and Thomas Counties. Grady and Thomas last had rust on kudzu in early 2006. Seminole, has rust for the first time this year. Rust was found in the county on volunteer soybeans in 2005. There are now eight counties in Georgia positive for rust in 2006.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=942

[Return to top]

Food Sector

26. *September 07, U.S. Food and Drug Administration* — **Mushrooms recalled.** Monterey Mushrooms of Watsonville, CA, is recalling approximately 10,000 cases of fresh sliced white mushrooms and fresh sliced baby bella mushrooms, because the mushrooms have the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Fresh sliced mushrooms were distributed from Monterey's location in Temple, PA, into Maryland, New Jersey, New York, North Carolina, Ohio, Pennsylvania, and Virginia through retail stores and produce market channels. No illnesses have been reported to date. Monterey received a positive test result for listeria on their Baby Bella product through a random product sampling by the Ohio State Department of Agriculture.
Source: http://www.fda.gov/oc/po/firmrecalls/monterey09_08.html

[Return to top]

Water Sector

27. *September 10, Reuters* — **Chemical leak poisons water supply in central China.** A sewage leak from a chemical plant has spilled the cancer−causing chemical arsenide into a river in central China's Hunan province, poisoning drinking water for nearly 100,000 locals, Chinese media said. Residents in Yueyang county were asked to stop drinking tap water and 18 fire engines distributed fresh water. Fresh water from a nearby reservoir was being discharged into the river in an attempt to dilute the polluted water. Hunan environmental authorities had detected arsenide levels in the Xinqiang river at ten times the normal standard, after the case was first reported on Friday, September 8. A chemical plant in Linxiang city, 30 miles upriver, was has been ordered closed after it was found leaking the toxin from its waste water pond.
Source: http://www.alertnet.org/thenews/newsdesk/PEK321505.htm

28. *September 07, Newslink Indiana* — **Well shut down after break−in.** A New Castle, IN, water well was shut down Friday, September 1, after it was discovered the locks on the enclosure gate and control box had been cut. Local investigators are treating the incident as a terrorist threat, since the source of the breach is unknown. Tests performed throughout the week show no contamination in the well. Water plant Superintendent Kenny Stockton said while the case is being treated as a contamination breach, he and other city officials believe copper theft was the

real motive for the break−in. The small amount of copper wire in the well's control box would have brought only a small amount of money at resale. In addition, the wire was live at the time of the break−in, running at about 480 volts, an issue that may have scared the thieves off. Because the city does not run all its wells at the same time, the shut−down did not interrupt water service to New Castle residents.
Source: http://www.newslinkindiana.com/news/00000010597.html

[Return to top]

Public Health Sector

29. *September 09, Agence France−Presse* — **World Health Organization confirms another bird flu fatality in Indonesia.** An eight−year−old girl who died last year has been confirmed as Indonesia's latest bird flu case, the World Health Organization (WHO) has said. The WHO said that the girl from Tangerang, a suburb on the outskirts of Jakarta, who died in July 2005, was Indonesia's 48th fatality. A recent revision in the way WHO confirmed H5N1 infection, meant that the girl, plus a 45−year−old man from central Java, who was infected last November but later recovered, had been recently confirmed as bird flu cases. The dead girl was the daughter of a 38−year−old man who was Indonesia's first laboratory confirmed human fatality of avian influenza, said the WHO. The girl's one−year−old sister, who died of severe pneumonia, was suspected of contracting the virus. At the time, however, health authorities had limited blood samples taken from the two sisters.
Source: http://news.yahoo.com/s/afp/20060909/hl_afp/healthfluindonesia_060909044005;_ylt=AuLy_XU3vZbvKzWOGFcBIu2JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

30. *September 08, Reuters* — **Horn of Africa states launch anti−polio drive.** Kenya, Somalia, and Ethiopia will vaccinate nearly three million children against polio in a bid to stamp out the paralyzing disease, which has re−emerged in the Horn of Africa. The vaccination campaign, which will run September 9−12, should be followed by two more in November and December in high risk areas around the borders between the three states. Polio−free for almost three years, Somalia became re−infected last year after the virus was brought in by people travelling from Yemen. With 215 confirmed cases, and with 14 out of its 19 regions infected, Somalia faces the toughest challenge in halting the spread of the disease. Ethiopia has reported 37 cases since polio reappeared in 2004. Kenya has been polio−free for 22 years and the campaign aims to prevent a return of the disease.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://za.today.reuters.com/news/NewsArticle.aspx?type=topNews&storyID=2006−09−08T064955Z_01_BAN824565_RTRIDST_0_OZATP−HEALTH−AFRICA−POLIO−20060908.XML

31. *September 08, U.S. Food and Drug Administration* — **Red Cross fined for failure to meet established blood safety laws.** The U.S. Food and Drug Administration (FDA) announced Friday, September 8, that the American Red Cross (ARC) is being fined $4.2 million for failure to comply with requirements under Federal laws and FDA regulations relating to the collection of blood products. These fines were assessed under an amended 2003 consent decree that calls for significant financial penalties when ARC fails to comply with FDA regulations and consent

decree provisions designed to ensure the safety of the nation's blood supply. The fines stem from a recently completed FDA review of recalls conducted by ARC between 2003 and 2005 that found these events were preventable by ARC. The violations include breaches of Good Manufacturing Practice regulations, such as a failure to ask appropriate donor screening questions and failure to follow manufacturer test protocols.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01447.html

32. *September 08, San Francisco Chronicle* — **West Nile warning system.** California cases of West Nile are down by two−thirds this summer −− an improvement gained in part with the help of thousands of citizens who filed dead bird reports. The California Department of Health Services has recorded 140 human cases of the mosquito−borne disease this season, compared with 500 at this time last year. Dead bird monitoring has become a critical tool in tracking the virus, which is lethal to dozens of avian species, particularly crows and jays. When birds are dying in big numbers, it's a good sign that mosquitoes infected with the virus are in the neighborhood and that human cases are likely to follow. Citizen bird spotters, sending their reports via the Internet or through a toll−free hot line, are helping state epidemiologists pinpoint viral hot spots. California has logged more than 40,000 reports of dead birds this season. Those reports are fed into a computerized map that displays where the avian death rate is suspiciously high. These digital "risk maps" serve as an early−warning system for local mosquito control districts, which then decide whether and where to spray pesticides that can knock down infected mosquitoes.
West Nile information: http://www.cdc.gov/ncidod/dvbid/westnile/index.htm
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2006/09/08/ BAGABL1ID51.DTL

33. *September 07, Emerging Infectious Diseases* — **Low frequency of poultry−to−human H5N1 virus transmission, Southern Cambodia, 2005.** To understand transmission of avian influenza A (H5N1) virus, researchers conducted a retrospective survey of poultry deaths and a seroepidemiologic investigation in a Cambodian village where a 28−year−old man was infected with H5N1 virus in March 2005. Poultry surveys were conducted within a close radius of the patient's household. Forty−two household flocks were considered likely to have been infected from January through March 2005 because more than 60 percent of the flock died, case−fatality ratio was 100 percent, and both young and mature birds died within one to two days. Two sick chickens from a property adjacent to the patient's house tested positive for H5N1. Villagers were asked about poultry exposures in the past year and tested for H5N1 antibodies. Despite frequent, direct contact with poultry suspected of having H5N1 virus infection, none of 351 participants from 93 households had neutralizing antibodies to H5N1. H5N1 virus transmission from poultry to humans remains low in this setting.
Source: http://www.cdc.gov/ncidod/EID/vol12no10/06−0424.htm

[Return to top]

Government Sector

34. *September 08, Department of Homeland Security* — **Fact Sheet: Protecting the Homeland Post September 11.** The Department of Homeland Security (DHS) has taken significant action to improve the nation’s security since the terrorist attacks of September 11, 2001. By improving security measures for the nation’s aviation system, implementing measures designed to protect

our critical infrastructure, using biometrics to establish and verify identity, strengthening border security, reflecting the lessons−learned from Hurricane Katrina, increasing the nation's preparedness for a disaster, and enhancing information sharing among federal, state, local, and international partners, DHS is leading the effort to protect the homeland. Information about this effort is available in the full text of this Fact Sheet.
Source: http://www.dhs.gov/dhspublic/display?content=5821

[Return to top]

Emergency Services Sector

35. *September 08, Associated Press* — **Wisconsin's ready for a terrorist attack.** Government and emergency officials in Wisconsin are much better prepared to respond to another terrorist attack −− or a natural disaster or infectious disease outbreak −− than before September 11, thanks to millions of dollars spent on planning, training, and new equipment and a new focus on preparedness. Since 9/11, the Department of Homeland Security has spent nearly $156 million in Wisconsin, according to the Governor Jim Doyle's Homeland Security Council. Doyle, in receiving a report Friday, September 8, from the state's homeland security adviser on Wisconsin's overall readiness, said enormous progress was made to prepare for emergencies. Among the progress Doyle cited was Wisconsin chapters of the American Red Cross training more than 2,100 new volunteers and the opening of a Wisconsin Statewide Intelligence Center to review and analyze data related to homeland security. La Crosse County Sheriff Michael Weissenberger said Wisconsin is safer because law enforcement and firefighters have received extensive new training. In addition, there is better communication between government agencies. State laboratories have also been beefed up to test materials more quickly and efficiently, and investigators have better equipment for detecting chemicals or biological agents.
Source: http://wfrv.com/topstories/local_story_251153909.html

36. *September 08, State of Illinois* — **Illinois: Significant improvements in interoperable communications.** Since the 9/11 terror attacks, Illinois has become a national leader in interoperable communications. Governor Rod R. Blagojevich directed the Illinois Terrorism Task Force (ITTF) to make interoperable communications for first responders a top priority, and in 2006 the task force began placing nine Illinois Transportable Emergency Communications Systems (ITECS) around the state, with a tenth ITECS headquartered with Emergency Management Agency in Springfield. The ITECS can be taken to a disaster scene anywhere in the state and used to patch together the different radio frequencies used by various response agencies. Other interoperable advances made include distribution of the following: STARCOM 21 700/800 MHz radios and digital VHF radios −− This equipment has been provided to all response agencies in Illinois to aid in responder communications; EMnet −− The ITTF provided each county emergency management agency and other public safety agencies with this satellite−based warning and alerting system; Medical Emergency Radio System of Illinois −− The ITTF provided these radios to all hospitals in each county; and Illinois Radio Emergency Assistance Channel −− The ITTF provided transmitters and equipment to the approximately 20 counties that did not have this interoperable system, which allows response agencies within that county to talk to each other during disasters.
Source: http://www.illinois.gov/PressReleases/ShowPressRelease.cfm?S

ubjectID=1&RecNum=5263

37. *September 07, Federal Emergency Management Agency* — **President declares major disaster for Arizona.** The head of the Department of Homeland Security's Federal Emergency Management Agency announced Thursday, September 7, that federal disaster aid has been made available for Arizona to supplement state and local recovery efforts in the area struck by severe storms and flooding during the period of July 25 to August 4.
For further detail: http://www.fema.gov/news/event.fema?id=7005
Source: http://www.fema.gov/news/newsrelease.fema?id=29658

[Return to top]

Information Technology and Telecommunications Sector

38. *September 08, eWeek* — **German researchers track latest MS06−040 worm attack.** Botnet hunters tracking the latest MS06−040 worm attack estimate that one malicious hacker earned about $430 in a single day by installing spyware programs on thousands of commandeered Windows machines. Security researchers at the German Honeynet Project discovered a direct link between the botnet−building attack and DollarRevenue, a company that pays between a penny and 30 cents per installation of its heavily criticized ad−serving software. Within 24 hours, the IRC−controlled botnet hijacked more than 7,700 machines via the Windows Server Service vulnerability and hosed the infected computers with the noxious DollarRevenue files. Thorsten Holz, a honeypot project founder, explained that a main IRC channel is being used to dispatch all incoming bots to join four different channels. The first sends instructions to propagate further by scanning for other vulnerable Windows machines. The second channel installs adware on all the machines, and a third was set up especially for the DollarRevenue installations. A fourth channel was used to install an additional binary on all bots. This is believed to be a spam proxy that can be rented out to spammers.
Source: http://www.eweek.com/article2/0,1895,2013924,00.asp

39. *September 08, Tech Web* — **Three years after Sobig.f, next attack cycle starting.** The upcoming third−year anniversary of the Sobig.f worm was marked Friday, September 8, by a security researcher who said its role in creating today's flood of phishing attacks and spyware means the next attack cycle will be even more virulent. Sobig.f, a worm that first appeared in August 2003 but which included a self−imposed cut−off date of September 10, 2003, was the first significant malicious attack loaded into an e−mail attachment, said Mark Sunner of security vendor MessageLabs. "The whole Sobig family was incredibly significant because that was the point where spam and viruses converged," said Sunner. Before that, the worst threats were self−replicating worms that attacked network vulnerabilities, such as 2003's MSBlast, or mass−mailed macro−based exploits like 1999's Melissa. "Today we're in the midst of the next wave of convergence, which will be all about spyware−type capabilities," said Sunner.
Source: http://www.techweb.com/wire/security/192700313;jsessionid=1FJP2WVW0ED2IQSNDLOSKH0CJUNN2JVN

40. *September 07, Register (UK)* — **Hackers are exploiting vulnerabilities in wiki software.** Software bugs in Pmwiki and Tikiwiki software applications are being actively used to create

botnets, the SANS Institute's Internet Storm Center reports. The Pmwiki exploit can only be exploited where the "Register_globals" attribute is enabled. However, the Tikiwiki exploit can be exploited regardless of this setting. As well as loading an IRC bot that connects to different channels to access to Undernet IRC servers, attackers are also loading a variety of other exploits and attack tools on the compromised machines. Alongside Perl flood scripts, useful for launching denial−of−service attacks, exploits for both 2.4 and 2.6 Linux kernels are also being loaded onto vulnerable machines.
Source: http://www.theregister.co.uk/2006/09/07/wiki_exploit/

41. *September 07, IDG News Service* — **Bug found in "classic" ICQ client.** AOL LLC is advising users of its ICQ instant message service to update to the latest version of the instant messaging software following the discovery of a bug in an older version of the product. Security researchers at Core Security Technologies Inc. reported Thursday, September 7, that they had discovered the flaw in ICQ Pro 2003b, a version of the ICQ client that AOL still offers for download, billing it as a "veteran version" of the product for users who prefer the earlier look−and−feel. Although the bug doesn't affect more recent ICQ software such as ICQ 5.1, it could mean serious problems for ICQ Pro 2003b users, according to Max Caceres, director of product management at Core, a vendor of penetration testing software. Core researchers have developed proof−of−concept code that causes ICQ Pro 2003b to crash and they believe that this vulnerability could eventually be exploited to run unauthorized software on a user's PC.
For further detail: http://www.coresecurity.com/index.php5?module=ContentMod&action=item&id=1509
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9003091&taxonomy Id=17&intsrc=kc_top

42. *September 07, Federal Trade Commission* — **Court halts illegal phone billing scheme.** A U.S. district court has entered an order barring unlawful activities by an operation that allegedly crammed unauthorized charges on the phone bills of small businesses or nonprofits for Website services that, in many cases, they didn’t know they had and didn’t request. The original complaint names defendants WebSource Media, L.L.C., BizSitePro, L.L.C., Eversites, L.L.C., Telsource Solutions, Inc., Telsource International, Inc., Marc R. Smith, Kathleen A. Smalley, Keith Hendrick, Steven Kennedy, John O. Ring, and James E. McCubbin, Jr. An amended complaint was filed later, adding defendant WebSource Media, L.P. The court has appointed a receiver to oversee the business operations and frozen defendants’ assets, pending trial. At trial, the Federal Trade Commission will seek a permanent halt to the operation’s activities and ask the court to order consumer redress for thousands of consumers who were illegally billed.
Source: http://www.ftc.gov/opa/2006/09/websource.htm

43. *September 06, Federal Trade Commission* — **FTC shuts down spyware operation.** An operation that placed spyware on consumers’ computers in violation of federal laws will give up more than $2 million to settle Federal Trade Commission (FTC) charges. The FTC said Wednesday, September 6, that it has obtained a settlement order against Enternet Media Inc., Conspy & Co. Inc., Lida Rohbani, Nima Hakimi, and Baback Hakimi, all based in California. The defendents distributed software called Search Miracle, Miracle Search, EM Toolbar, EliteBar, and Elite Toolbar. According to the FTC’s complaint, the Websites of the defendants and their affiliates caused “installation boxes” to pop up on consumers’ computer screens. In one variation of the scheme, the boxes offered a variety of “freeware,” including music files,

cell phone ring tones, photographs, wallpaper, and song lyrics. In another, the boxes warned that consumers' Internet browsers were defective, and offered free browser upgrades or security patches. Consumers who downloaded the supposed freeware or security upgrades did not receive what they were promised; instead, their computers were infected with spyware that interferes with the functioning of the computer and is difficult for consumers to uninstall or remove.
Source: http://www.ftc.gov/opa/2006/09/enternet.htm

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 57715 (−−−), 445 (microsoft−ds), 32797 (−−−), 113 (auth), 4662 (eDonkey2000), 6346 (gnutella−svc), 139 (netbios−ssn), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

44. *September 11, CNN* — **Al Qaeda releases 9/11 anniversary message.** A lengthy video statement from Ayman al−Zawahiri, issued on the eve of the fifth anniversary of al Qaeda's attacks on the United States, calls on Muslims to step up their resistance to the United States and warns that "new events" are on the way. It appeared just hours before Monday's anniversary of the al Qaeda 2001 attacks on New York and Washington. The statement calls on Muslims to fight U.S. allies in Somalia, where an Islamic militia recently pushed an American−backed alliance of warlords out of the capital Mogadishu. It also urges them "to make use of every opportunity afforded him to take revenge on America" for the imprisonment of blind Egyptian cleric Omar Abdel Rahman, considered a major theological force behind al Qaeda. CNN terrorism analyst Peter Bergen said Sunday, September 10, that al Qaeda was certain to make some sort of statement on Monday's anniversary.
Source: http://www.cnn.com/2006/US/09/11/zawahiri.911/index.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer